ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operations and Maintenance

of

Safety Instrumentation Systems

ProSalus Limited

Slide 8 - 1

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Using the Safety Instrumented System

- Installation and commission – IEC 61511 Clause 14
- Validation – IEC 61511 Clause 15
- Operation & Maintenance – IEC 61511 Clause 16
- Modifications – IEC 61511 Clause 17

ProSalus Limited

Slide 8 - 2

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61511 Safety life-cycle goals (Clause 6.2.3)

1. ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
2. ensure proper installation and commissioning of the safety instrumented system;
3. ensure the safety integrity of the safety instrumented functions after installation;
4. maintain the safety integrity during operation (for example, proof testing, failure analysis);
5. manage the process hazards during maintenance activities on the safety instrumented system.

ProSalus Limited

Slide 8 - 3

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Installation and Commissioning

- **Installation and commissioning must be**
  - **Carried out according to plan**
  - **Documented Evidence of**
    - **Installation and commissioning activities**
    - **Failure resolution**
    - **Retest**

ProSalus Limited

Slide 8 - 4

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Installation and Commissioning

- **System / Equipment Suppliers**
  - Supply documentation as per 61508 / 61511 requirements to ensure SIS is installed and commissioned correctly
- **Operators**
  - Follow Installation and Commissioning Plan
  - Tested in accordance with Commissioning Procedure
  - Safety Manual requirements included in O&M Procedures

ProSalus Limited

Slide 8 - 5

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Validation Plan

- **Operator Requirement to assure**
  - **Integrity requirement achieved**
  - **Functional requirements achieved**
  - **Basis of validation is the safety requirements specification**

ProSalus Limited

Slide 8 - 6

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Validation Report

- **Documented Evidence of:**
  - **Validation activities completed**
  - **All Safety Instrumented Functions validated**
  - **Tools used during validation**
  - **Results of the validation**
  - **Any discrepancies**
    - **SIS Fit for Purpose**

ProSalus Limited

Slide 8 - 7

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The SIS Validation activities must include as a minimum the following:

- SIS performs in all operating modes as identified in the SRS;
- Confirmation that adverse interaction of the BPCS and other connected systems do not affect the proper operation of the SIS;
- SIS properly communicates (where required) with the BPCS or any other system or network;
- Sensors, logic solver, and final elements perform in accordance with the SRS;
- SIS documentation is consistent with the installed system;
- Confirmation that the SIF performs as specified on invalid process variable values;
- The proper shutdown sequence is activated;
- The SIS provides the proper annunciation and proper operation display;

ProSalus Limited

Slide 8 - 8

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

The SIS Validation activities - continued:

- The SIS reset functions perform as defined in the SRS;
- Bypass functions operate correctly;
- Start-up overrides operate correctly;
- Manual shutdown systems operate correctly;
- The proof-test intervals are documented in the maintenance procedures;
- Diagnostic alarm functions perform as required;
- Confirmation that the SIS performs as required on loss of utilities (for example, electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the SIS returns to the desired state;
- Confirmation that the EMC immunity, as specified in the SRS, has been achieved.

ProSalus Limited Slide 8 - 9

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operation and Maintenance

- Key to maintaining the SIL over plant life time
- O&M procedures must include Safety Manual requirements
- Estimated repair times included in SIL verification
- Proof Test Intervals included in SIL verification
- Critical to plant safety that these are completed to schedule

ProSalus Limited Slide 8 - 10

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Operator Requirements

- Procedures in place for
  - SIF Maintenance
  - Repair activities
  - Change control / modifications
  - Functional Safety Assessment
- Periodic Functional safety audits

ProSalus Limited

Slide 8 - 11

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Modification Documentation

- Documentation includes
  - The modification or retrofit request
  - The impact analysis
  - Re-verification and re-validation of data and results
  - All documents affected by the modification and retrofit activity

ProSalus Limited

Slide 8 - 12

Functional Safety Engineering

Impact Analysis

- An impact analysis includes
  - An assessment on what impact the change has
  - Hazard and risk analysis to applicable phases of the lifecycle
  - Guarantee of functional safety at all times
  - Result of the impact analysis determines whether the modification will be authorized

ProSalus Limited Slide 8 - 13

Functional Safety Engineering

Override Procedures

- Maintenance overrides are not problem as long as you guarantee the safety function
- Things to think about
  - Is there a procedure?
  - Are people informed?
  - Is the override time limited?
  - Do you lock out/tag out the area?

ProSalus Limited Slide 8 - 14

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Why do proof testing?

Keeps the PFD within the design targets

OHSA requirements in USA

IEC 61508 and 61511 compliance

PFDavg increases with test interval …so without testing the PFDavg rises above limits and SIL falls to ZERO.

ProSalus Limited

Slide 8 - 15

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Proof testing: Key points

- Use a documented procedure
- Test entire SIF
- Test intervals based on the Safety Requirements Specification
- Review the test interval after operational experience
- Full testing after any changes
- Description of all tests performed
- keep records to certify the tests and inspections have been performed.

ProSalus Limited

Slide 8 - 16

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Valve on-line testing methods

- Problem is to test the ability of the valve to close off flow or release pressure as per function
- The need for final process test may be reduced if duty levels are not severe.
- The testing of solenoid and ability to move the valve covers a large portion of potential faults.
- Partial closure testing (Tia = PTI/10) and physical inspections at higher frequencies , leaving full closure tests to once per year or greater.
- Define the testing facilities needed during the design stage.

ProSalus Limited

Slide 8 - 17

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Inspection Programme guidance from IEC 61511 Part 2

16.3.2 Inspection

As stated in IEC 61511-1, inspecting the SIS is different from proof testing. Whereas a proof test is ensuring the SIS will operate properly, a visual inspection is required to validate the mechanical integrity of the installation.

Normally, the inspection is done at the same time as the proof test but it may be done at a more frequent interval if desired..

ProSalus Limited

Slide 8 - 18

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Maintenance Management Programme (IEC 61508)

Some useful guidelines in these standards on how maintenance response and reporting activities can assist in building an accurate record of SIS reliability.

From Phase 14 of the safety life cycle model in IEC 61508-1 see next 3 diagrams, based on fig 7, 8 and 9

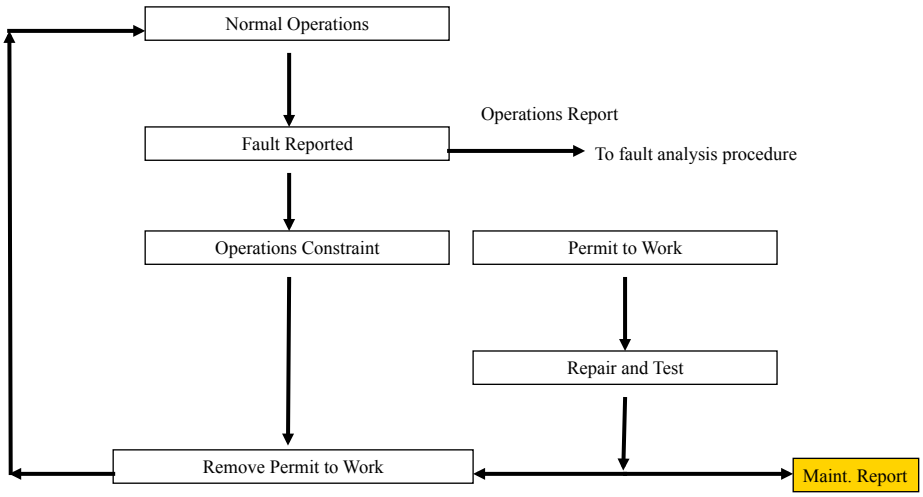
These procedures lead to analysis of performance problems and may lead to modifications. Management of change M.O C. procedures then apply…see following slides

ProSalus Limited Slide 8 - 19

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Revealed faults procedure: response to reported fault.

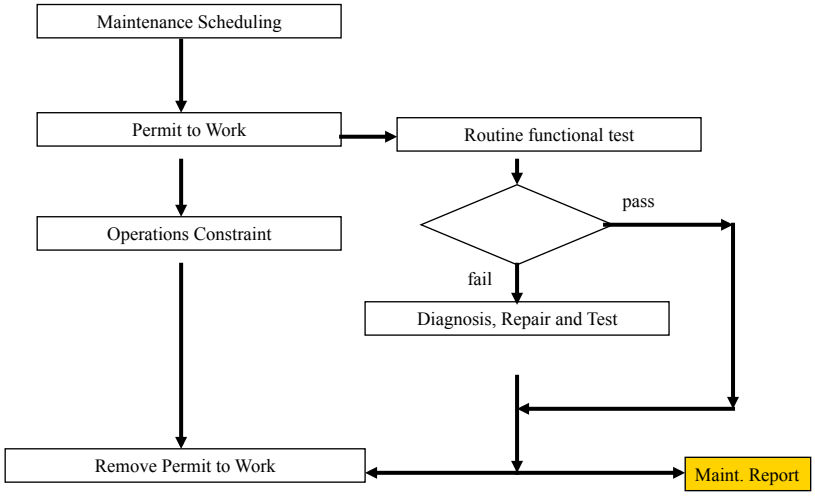


ProSalus Limited Slide 8 - 20

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Unrevealed faults procedure: Proof testing



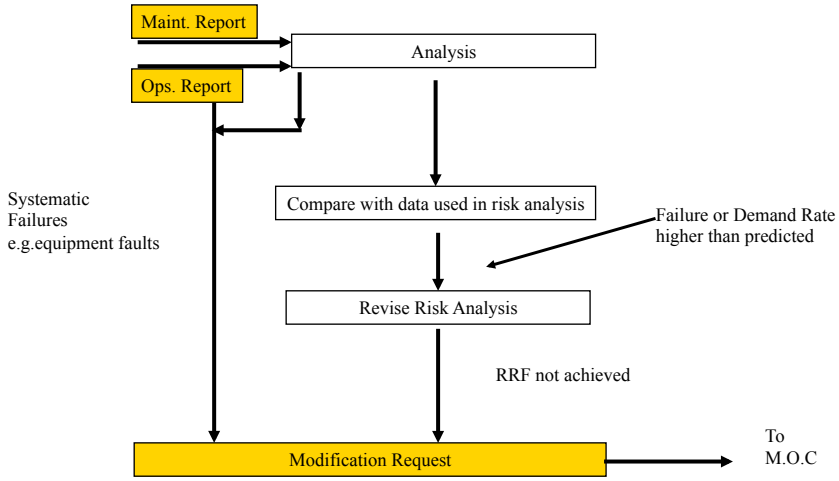
ProSalus Limited

Slide 8 - 21

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Evaluation of maintenance and proof testing reports



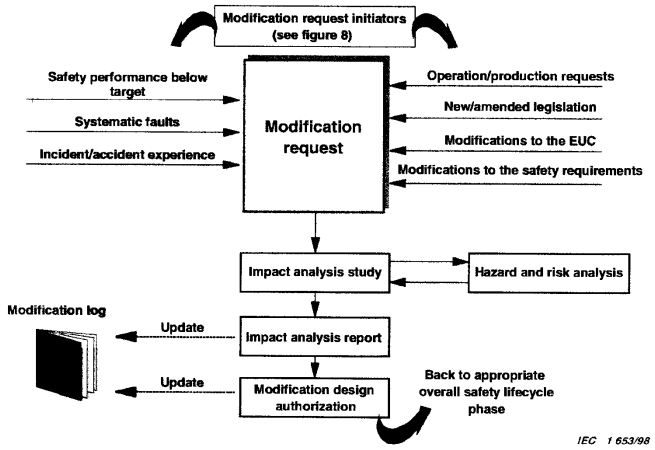
ProSalus Limited

Slide 8 - 22

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

IEC 61508 Modification Procedure Model



ProSalus Limited

Slide 8 - 23

ProSalus SAFETY CONSULTANTS

Functional Safety Engineering

Summary

- Management of Change critical to Process Safety
- MOC and Maintenance is a Key Performance Indicator
- Proof Test Integral to maintaining SIL Capability

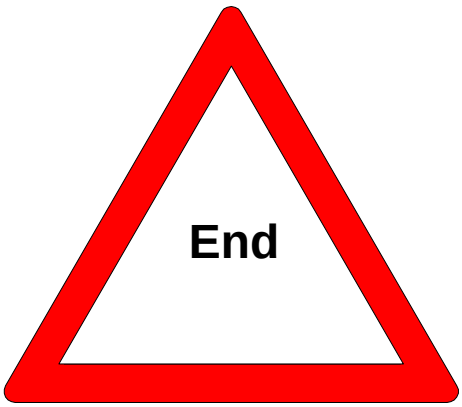
Thanks for your attendance and any Questions

ProSalus Limited

Slide 8 - 24

ProSalus
SAFETY CONSULTANTS

Functional Safety Engineering



ProSalus Limited

Slide 8 - 25